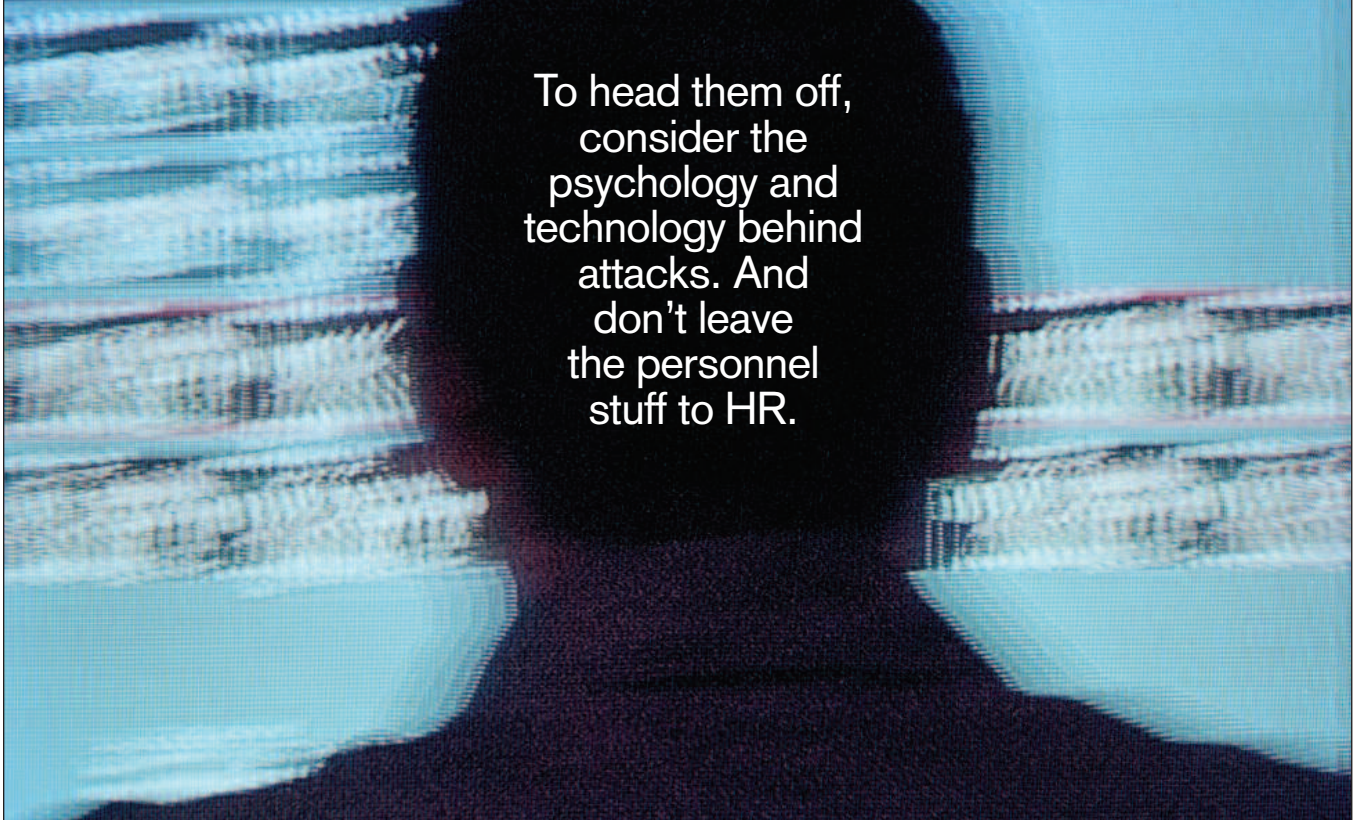


Insider Threats



To head them off, consider the psychology and technology behind attacks. And don't leave the personnel stuff to HR.

By Larry Greenemeier

ROGER DURONIO faces up to eight years in a federal prison when he steps before a judge this week to be sentenced for sabotaging UBS Paine-Webber's IT systems in 2002. If you think there are no potential Duronios in your organization, consider this a brief history lesson on tech employees gone bad, and a refresher course on how to identify and stop insider malcontents before they do some serious damage.

As a system administrator, Duronio, convicted this summer, placed a "logic bomb" to knock out much of UBS's network, then made financial bets that would pay off if the company's stock tanked as a result. A former VP of IT at SourceMedia, Stevan Hoffacker, was arrested in mid-November on charges he hacked into his former company's e-mail system so he could warn people still working there that they were going to be laid off. Prudential Insurance IT staffer Donald

McNeese in 2002 stole records from a Prudential database containing information on about 60,000 employees and was caught trying to sell identities for credit card fraud.

Nearly two-thirds of the 616 security pros surveyed this year by the Computer Security Institute say insiders account for some portion of the financial losses their organizations experience because of breaches. Some 39% of respondents attribute more than 20% of their organizations' financial losses to insider attacks, while 7% estimate that insiders account for a whopping 80% of financial losses.

Insiders aren't the most common security problem, but they can be among the most costly and the most damaging to a company's reputation. Insider attacks against IT infrastructure are among the security breaches most feared by both government and corporate security pros, says Eric Shaw, a psychologist and former CIA intelligence officer

NEWS & ANALYSIS

who has studied insider threats the past decade.

What to do? The risks can be lessened first by doing background checks on potential IT employees—something far more companies are doing this year, according to Carnegie Mellon University's CERT (see story below). If an employee is terminated, it's crucial that all system access be revoked immediately. It sounds obvious, but that doesn't mean it's always done. About half of all insider attacks take place between the time an IT employee is dismissed and his or her user privileges are taken away, says Dawn Cappelli, a senior member at the CERT Coordination Center, part of Carnegie Mellon's Software Engineering Institute.

When it comes to current employees, IT managers must do something they might not have a taste for: Keep an eye out for insubordination, anger over perceived mistreatment, or resistance to sharing responsibility or training colleagues—all warning signs someone may be capable of system sabotage or data theft. "The biggest misconception about preventing insider attacks is that IT needs to worry only about technology issues and HR has to worry only about personnel issues," Cappelli says.

Defending against insiders isn't easy, but knowing what to look for and understanding who you're up against certainly helps, says Shaw, who co-authored a report last year titled, "Ten Tales Of Betrayal: The Threat To Corporate Infrastructures By Information Technology Insiders."

IT managers must be watchful any time someone with access to sensitive systems has a falling out with his or her bosses. That's what happened with Duronio, who was upset his bonus fell about \$15,000 short of his expectations. It's also the story of Claude Carpenter, who worked for government contractor Network Resources doing part-time systems administration on three Internal Revenue Service servers. In May 2000, suspecting he'd be fired after a dispute with a co-worker, Carpenter inserted several lines of code that would command the three servers under his care to wipe out data if network traffic reached a certain level. He tried to conceal his activities by turning off system logs and removing history files, but he aroused colleagues' suspicion by

calling several times during the next two weeks to ask "if the machines were running OK" and "if anything was wrong with the servers," says a July 2001 Justice Department description of the case. Carpenter was sentenced to 15 months in prison and ordered to pay \$108,800 in restitution.

Managers must not only monitor system access, but also let employees know their system changes can be tracked. Employers should be wary of people unwilling to share their knowledge about systems or uncomfortable with the fact that their activities accessing systems or data can be tracked.

One related element: Make sure each IT worker has just enough system access to get his or her job done. "Usually, a person who does damage was given more access than they needed," says Bill Moylan, senior director of Aon Consulting's IT risk consulting group, who spent 25 years with Long Island's Nassau County Police Department. One financial services CIO makes that point by not giving himself data center access, since he doesn't need to be in there to do his job. Access can be something of a status symbol, so don't wait for IT staffers to complain they have too much, Moylan says.

This is the CIO's problem to solve. Though technology is everywhere in companies, system attacks are nearly all driven by scoundrels working in IT who have the knowledge and access to pull them off. A recent survey by the Secret Service and CERT Coordination Center/SEI indicates that 86% of internal computer sabotage incidents are perpetrated by tech workers.

The rise of identify theft and the heightened sensitivity around customer and employee data have raised the stakes. One of the first insider cases to drive this point home was that of former Prudential database administrator McNeese, who was charged with identity theft, credit card fraud, and money laundering for stealing records from a Prudential database. He even sent e-mails to victims, trying to incriminate his former boss. McNeese received three years' probation, was ordered to pay \$3,000 in restitution, and was required to get psychiatric treatment.

Insider Profiles

Almighty Creator Tim Lloyd disliked sharing info about systems he built—and left code to knock them out when he got fired.

■ **Mad Bomber** Sure he'd soon be fired, Claude Carpenter put a code bomb on IRS servers.

■ **Prolific Reader** Stevan Hoffacker is accused of accessing ex-employer's e-mail to learn who'd be fired.

■ **Paybacker** Mad about a bonus shortfall, Roger Duronio brought down employer's system.

Multifaceted Malcontent Donald McNeese tried to sell employee data he stole. But he seemed as intent on embarrassment—trying to frame his boss and planting info on sex Web sites.

Employees most likely to commit insider theft or sabotage share a number of characteristics, which can include mental health disorders, personalities that clash with authority, and a history of behavioral violations in the workplace, often documented by HR, says Shaw, who has worked as a consultant to the Defense Department profiling characteristics of insiders who commit computer crimes.

Other clues are less academic but no less important. Simply getting to know employees will create loyalty and may even tip off potential problems. "If a guy on your staff needs an extra \$20,000 to pay for his kid's college tuition, he might try to sell credit card numbers," says David Giambruno, VP of global service delivery for cosmetics company Revlon and formerly the director of engineering, security, and deployment at Pitney Bowes.

GET PROACTIVE

Technology also plays a key role in thwarting insider attacks. Giambruno believes in encrypting data that "could remotely be seen as sensitive." Revlon encrypts sensitive data in applications and databases using Ingrian Networks' DataSecure network appliance, with its built-in encryption software and middleware for connecting to servers. Giambruno advocates creating an audit trail, where employees who want access to encrypted data have to state their reasons and get executive sign-off on the decryption key. By encrypting data, he says, "you take away the low-hanging fruit for insiders."

Risk management software and services can help, too. IBM last week announced plans to buy Consul Risk Management and add Consul's products to the Tivoli line of IT management software. Consul and rival risk management offerings from Elemental Security and others are designed to alert IT managers when data or systems are improperly accessed,

whether from the outside or by staffers.

Technology plays a vital role when an IT worker is fired. Immediately cutting network, system, and data access privileges is only the start. If there's a reason for concern, managers should, ideally before termination, audit projects the employee worked on to understand his or her access privileges and look for back-door access programs they may have created in anticipation of being fired. "Termination doesn't end the risk," Shaw says. "It probably just escalates it."

If you doubt such steps will be enough to deter angry IT employees, Shaw suggests laying it on the table that you'll be keeping tabs on them. "Hold something over the former employee's head, such as their severance package or continued benefits," he says. "Let them know that if you see any problems with your IT systems, you'll have the police pay them a visit."

Sound like the kind of stuff you'd prefer to let HR handle, so you can get back to working with your talented, trusted employees? When it comes to insider threats, IT departments must accept that they're the first line of defense, with HR as their closest partner, CERT's Cappelli says. "They need to have an understanding of both the psychology and the technology behind these attacks to prevent them from happening," she says.

Great, like IT managers need another hat—now they're psychologists. But it's true that all IT pros are in this together against the rotten few, whether the rogue who's "just" peeking at documents he shouldn't access or the saboteur who's knocking out a company on which tens of thousands depend for their livelihoods. Thwarting them—and keeping the respect and trust an entire profession has earned—is what's at stake. —WITH SHARON GAUDIN

Write to Larry Greenemeier at lgreenem@cmp.com. Visit our Security Tech Center: informationweek.com/security